Office de la propriété intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An Agency of Industry Canada

#2

Bureau canadien des brevets
Certification

Canadian Patent Office
Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawing, as originally filed, with Application for Patent Serial No: **2,315,933,** on August 14, 2000, by **IBM CANADA LIMITED - IBM CANADA LIMITÉE,** assignee of Weidong Kou, for "Method and System for Granting Access to Information for Electronic Commerce".

CERTIFIED COPY OF PRIORITY DOCUMENT

Agent certificateur/Certifying Officer

November 1, 2000

Date

Canada

(CIPO 68)

OPIC CIPO

Method and System for Granting Access to Information for Electronic Commerce

Abstract

The present invention provides a method and a system that enables an information provider or a vendor to manage group-assigned information, and control access to the information using a reduced number of encryption/decryption keys are used for protecting the information so that that information handling devices are not overburdened. The information could contain pricing, warranty, and other suitable information. An aspect of the invention provides a controlled access catalog accessible by members of authorized groups. The following is stored: identification of authorized groups; identification of selected catalog items and group information for the authorized groups; a private key for each authorized group for encrypting group information for each group respectively; a public key for each authorized group for decrypting encrypted group information, the public key corresponding respectively to the private key of the authorized group; and, an authenticator for granting access to the public key of each authorized group for decrypting encrypted group information for members of the authorized groups.

Method and System for Granting Access to Information for Electronic Commerce

Field of the Invention

The present invention relates to a method and a system for granting access to information to customers over a communications network, and more specifically to a method and system for granting access to group-targeted, protected information to members of customer groups over a network of computing devices.

Background of the Invention

For an e-commerce vendor, the ability to grow and respond quickly is a distinctive and important business advantage in today's fast-moving marketplace. The pressure to respond quickly is driven by many factors, such as: identifying new business opportunities, improving customer service, reducing purchasing and sales costs, and reducing inventories. The vendor must continuously strive to improve business and technological issues that surround granting access to information. Maintaining a leading position within the marketplace requires a vendor to establish and refine effective business models to increase profits, and ensure trusted and secured financial transactions and exchange of confidential information.

It is an important competitive advantage to quickly and easily grant selected or controlled access to confidential information to customers over a communications network such as the Internet. For example, to overcome a short-term competitive threat, a vendor may need to quickly provide information to customers in which the information may be time-sensitive or valid for specific market conditions. Content of the information could represent negotiated

pricing, discounted pricing, important notices such as press releases, or warranty information. The information is used to influence purchasing decisions of customers while quickly managing requests from potentially many customers via the Internet, and while minimizing computing hardware configuration and cost.

Protecting information can be accomplished by using symmetric encryption in which a single key is used for encrypting and decrypting information, or asymmetric encryption based on public-private key pair cryptography in which a public key is used for encrypting information and a private key is used for decrypting encrypted information; however, a significant problem occurs in using keys when a potentially very significant number of keys are to be managed. Certificate Authorities (CAs) are used to register and contain public keys that belong to users. A user registers with a CA to obtain a certificate that contains the public key of the user. A certificate is digitally signed by a CA, which is subsequently placed into a public directory, such as a CCITT X.500 directory. Typically, a CA manages a directory. When user A wants to send a confidential electronic message to user B, user A locates a certificate that belongs to user B by examining a directory; then, user A encrypts a message by using a public key that belongs to user B, in which the public key can be found in a certificate that belongs to user B. Then, user A sends an encrypted message to user B. Only user B has access to a private key that belongs to user B, in which the private key is used to decrypt the encrypted message. It is understood that all private keys remain inaccessible to nonowners to ensure message security, while all public keys are shared. In an e-commerce application, a vendor cannot assume that customers are registered with a CA. In addition, CAs may not wish to share directories with other CAs. Since a public key infrastructure may not be available, a vendor must directly manage keys for customers.

Assigning a unique pair of keys to each customer would require managing a very large number of keys, which would require additional processing effort and computer hardware configurations when attempting to manage many requests for access to information.

Sirbu et al -- in US 5,809,144 "Method and Apparatus for Purchasing and Delivering Digital Goods over a Network" dated 15 September 1998 -- discloses a method for purchasing and delivering digital goods over a network. This reference apparently uses symmetrical encryption which requires managing a very large number of keys (one key is used per delivered electronic document). This reference apparently suggests that a vendor must use a different key when delivering another electronic document to a customer to prevent the customer from opening a received, unpaid document by using a previously received key. A significant number of keys would be required since each unit of information is individually protected. It would be a significant advantage and improvement if a solution could use a small number of keys for protecting information for access by a very large number of customers.

Carter -- in US 5,787,175 "Method and Apparatus for Collaborative Document Control" dated 28 July 1999 -- discloses a method for distributing a document within a class of authorized users by enabling access of the document from within a portion of the document in which the users encrypt and decrypt portions of the document and each user has a unique public-private key pair. This reference apparently uses a very large number of keys to grant access to information to a significantly large number of customers.

Linehan et al -- in US 5,495,533 "Personal Key Archive" dated 27 February 1996 -- discloses a method for managing encryption keys that are used for encrypting data files. This reference apparently uses symmetric encryption keys such that each key is correspondingly

assigned to a document for which a dedicated key server automatically manages all of the keys for the documents and the documents are managed by a document server. This reference apparently requires using additional computer hardware configurations. It would be a significant advantage to use a minimal number of keys to minimize hardware configuration and processing effort required for granting access to information to a significantly large number of customers.

Hass et al -- in US 5,719,938 "Methods for Providing Secure Access to Shared Information" dated 17 February 1998 -- discloses a method for using symmetrical cryptographic systems. This reference apparently requires a vendor to manage a very large number of encryption keys, and to create encrypted information for each customer every time a customer requests access to information. This reference apparently presents a significant processing burden when attempting to manage a large number of customers, which would be a disadvantage when attempting to respond quickly to fast-changing marketplace conditions.

Lohstroh et al -- in US 5,953,419 "Cryptographic File Labelling System for Supporting Secured Access by Multiple Users" dated 14 September 1999 -- discloses a method for protecting data by assigning one key per user. Each authorized user uses a unique private key to gain access to encrypted portions of the file. This reference apparently requires generating and managing a significantly large number of keys for granting access to information to a large number of customers.

Therefore, a solution would have to enable a vendor to quickly and easily grant access to protected information to many customers while minimizing computer configuration and processing effort.

Summary of the Present Invention

One aspect of the present invention provides a method and a system for managing access to information in a catalog to customers over a network which protects the information and reduces computing effort and hardware requirements. Protection preferably includes encryption such as key-based cryptography and the like for preventing unauthorized access to information. Another aspect of the present invention also reduces effort for managing information by classifying customers into groups in accordance with a type of relationship a vendor wishes to define with members of a group and creating information that is assigned to specific groups of customers. An aspect of the present invention reverses normal usage of public-private key pairs to significantly reduce work related to managing encryption keys as will be explained below.

The prior art requires a vendor to create protected or encrypted pricing for individual customers in which as the number of customers increases, using prior art techniques, a vendor would face a significant storage and processing burden because of the activity associated with managing keys. The present invention manages access to information to groups of customers, which would be relatively small in number compared to a total number of customers, and assigning protected information to each group as will be explained hereunder.

A preferred embodiment of the present invention provides a controlled access catalog for storing identification of catalog items accessible by members of authorized groups. The catalog includes: identification of authorized groups; identification of selected catalog items and group information for the authorized groups; a private key for each authorized group for encrypting group information for each group respectively; a public key for each authorized group for decrypting encrypted group information, the public key corresponding respectively to the private

key of the authorized group; and, an authenticator for granting access to the public key of each authorized group for decrypting encrypted group information for members of the authorized groups.

Preferably the authenticator, which will be implemented in software, is responsive to receiving member identification for granting access to the public key of an authorized group.

For providing restricted access to pricing, the group information may include group pricing.

The catalog can include identification of members of each authorized group to be used in authentication. An encryptor such as encryption software can be used for encrypting the group pricing by using the private key.

An access interface can be provided for accessing the encrypted group pricing of authorized groups by their members. The access interface is responsive to a member providing identification and authentication data for confirming authorization to access encrypted group pricing.

In another implementation, a multinodal information-handling network includes the catalog at a node of the network.

A user interface is provided at another node of the network, the user interface includes: an input for accepting member input, including member identification and authentication data; and, a communication interface for sending member input to the catalog over the network.

The communication interface is preferably adapted to receive information output from the catalog including identification of catalog items and decrypted group pricing. The user interface includes a display, for a user, to view identification and pricing of catalog items. The display can be used to present to a user: an input screen having an input field for the user to enter a query including member identification and authentication data to be sent to the catalog by the

communication interface to request access to the catalog; and, a user presentation screen to display information including decrypted pricing of catalog items available to the user after access to the catalog has been communicated to the communication interface.

Another aspect of the present invention provides a method for managing a controlled access catalog for storing identification of catalog items accessible by members of authorized groups by: storing identification of authorized groups; storing identification of selected catalog items and group information for authorized groups; encrypting group information with a private key of each authorized group; storing a public key for each authorized group for decrypting encrypted group information, the public key corresponding to the private key of each authorized group; and, authenticating and granting access to the public key of an authorized group for decrypting encrypted group information for members of that authorized group.

The step of authenticating is preferably responsive to receiving member identification, for granting access to the public key of an authorized group.

The method can include decrypting encrypted group pricing using a public key of an authorized group when pricing information is requested by an authenticated member of the authorized group.

Storing identification of members of an authorized group can preferably be stored by the catalog.

The method of the invention can include: encrypting group pricing of an authorized group by using the private key of the authorized group; and, providing access to encrypted group pricing of an authorized group in response to a user providing identification and authentication data for confirming authorization of the member to access encrypted group pricing.

Another aspect of the present invention provides a program product having a computer-readable medium for storing computer-readable program code for managing a controlled access catalog accessible by members of authorized groups. The program code includes: computer-readable program code for causing the computer to store identification of authorized groups; computer-readable program code for causing the computer to store identification of selected catalog items and group information, which may include group pricing, for the authorized groups; computer-readable program code for causing the computer to encrypt the group information for each authorized group with a private key of the authorized groups; computer-readable program code for causing the computer to store public keys for the authorized groups for decrypting encrypted group information, the public keys corresponding respectively to the private keys of the authorized groups; and, computer-readable program code for causing the computer to authenticate and grant access to the public keys of authorized groups for decrypting encrypted group information for members of the authorized groups.

The program product may advantageously have computer-readable program code for causing the computer to decrypt encrypted group pricing using a public key of the group when pricing information is requested by an authenticated member of an authorized group.

Additionally, the program product preferably includes: computer-readable program code for causing the computer to encrypt the group pricing of an authorized group by using the private key of the authorized group; and, computer-readable program code for causing the computer to access the encrypted group pricing of the authorized group by the members, responsive to a member providing identification and authentication data for confirming authorization of the member to access the encrypted group pricing.

Detailed Description of the Drawings of the Present Invention

To illustrate the aspects of the present invention, the following figures are used, in which:

Fig. 1 shows a process for how a customer (who is a member of an authorized customer group) is granted access to protected pricing information managed in a controlled access catalog; and,

Fig. 2 shows a flow chart for controlling access to pricing information on a web server.

Detailed Description of the Preferred Embodiments of the Present Invention

The present invention will be described with reference to an exemplary context of a method and system for granting access to members of customer groups to pricing information that is assigned or intended for viewing by the members of customer groups over a network. The present invention could be adapted to operate over many types of communication networks or to grant access to any suitable type of information. An information owner or controller such as a vendor may create information that has a pricing content in which pricing information is assigned to specific customer groups such as wholesale pricing for a wholesale customer group. It can be appreciated that the information could be warranty information and the like that is assigned to members of a predetermined customer group. However, for the purposes of describing aspects of the present invention, this example will use information that has a pricing content.

The method of the present invention allows an information owner or a vendor to grant access to pricing information that is assigned to specific groups of members, in which content of

the information revealed depends on the group to which a member belongs. Information could reside in software databases and applications that are implemented on web servers or other information handling devices. A preferred embodiment of the present invention uses asymmetrical encryption based on public-private key cryptography in which it is preferred that each public-private key pair is correspondingly assigned to each customer group. Public and private keys are used to encrypt and decrypt the information so that a simplified computer configuration can be implemented. The present invention does not correspondingly assign each key pair to each customer to prevent overwhelming a simple computer configuration and thereby avoids complicated computer-hardware configurations. An aspect of the present invention uses public-private keys in a reverse sense compared to traditional use of public-private keys as taught in the prior art as will be shown below.

It can be appreciated that an information provider or a vendor would deal with many different customer groups such as wholesale customers, retail customers and the like. Therefore, it would be advantageous for a vendor to manage pricing information so that pricing content is assigned for access by members of predetermined customer groups. There would be many situations in which this is desirable, such as:

- To show appreciation to customers that have buying patterns that could be characterized as long term, high-volume, or repeat in which a vendor may want to offer favourable or discounted pricing to these types of customers;
- To attract new customers, a vendor may want to offer a special one-time or time-limited pricing to new customers; or

- To focus special attention on a large-volume customer which purchase a significant portion of a vendor's revenue, the vendor may want to offer mutually negotiated pricing, while other groups of customers are offered non-negotiated pricing.

Therefore, it is an advantage for a vendor to implement pricing that is structured or targeted to specific groups of customers in which the vendor avoids managing specific pricing for specific customers. In this manner, groups of customers could obtain access to group-targeted pricing that is assigned to a group of customers. Content of the pricing could be a reflection of a type of relationship a vendor desires to have with specific groups of customers. The strategy would be then to enable a vendor grants access to group-encrypted, group-targeted pricing along with a group-targeted decryption for decrypting the encrypted pricing.

A vendor begins by defining specific groups of customers into which customers are assigned. For example, let N be a number of customer groups in which N = 3. A vendor will want to define three pricing strategies for either a product or a range of products in which a wholesale pricing strategy is assigned to a wholesale customer group, a retail pricing strategy is assigned to a retail customer group, and a favorable pricing strategy is assigned to a favorable customer group so that the pricing strategies are assigned to each customer group. It can be appreciated that it may be possible to assign group-targeted pricing to more than one group which may provide improved flexibility and convenience for managing customer relations. This example is further developed into two scenarios, namely:

- Scenario (A) in which a vendor wants to protect all three pricing strategies from unauthorized access from any unregistered customers or from members of a another group; and

- Scenario (B) in which a vendor wants to allow a retail pricing strategy to be seen by anybody who can access their web sever but to protect the remaining pricing strategies from unauthorized access.

For scenario (A), customers will be initially required to register with a vendor's web server. Upon successful registration, each customer could be assigned an identification such as an ID and the like, and an authentication such as a password and the like for identifying and authenticating customers so that only authenticated members of groups are granted access to group-targeted pricing and a group-targeted decryption . Prior to providing access to protected pricing, a vendor assigns each customer to a specific group or to a range of groups so that a customer is a member of at least one group. In this example, a vendor uses three different public-private key pairs in which each key pair is assigned to each customer group. It can be appreciated a key pair could be assigned to more than one group which may provide improved flexibility and convenience for managing customer relations. After performing an identification and authentication step, authenticated members of a group will be given access to an assigned public key along with group-encrypted, group-assigned pricing. Preferably, before members obtain access to assigned pricing, the vendor could encrypt specific pricing assigned to each group by using a private key that corresponds to each group. Also, before a customer is granted access to any group-targeted, protected pricing, a web server could identify and authenticate a customer by evaluating the customer's submitted ID and authentication password. It can be appreciated that a unique ID and password could be assigned either to each specific customer or could be assigned to each customer group (i.e., a group-oriented ID and password). After

successfully identifying and authenticating a customer, a web server determines to which customer group that a member belongs, and then grants access to:

- Encrypted pricing that is assigned to a group in which a customer is a member; and
- A public key that is assigned to a group that a customer is a member so that the public key can be used to decrypt encrypted pricing so that a content of the pricing can then be displayed to the customer via a web browser.

It is preferable to configure the present invention so that unauthenticated customers are prevented from accessing encrypted pricing along with any corresponding decryption key, which could be realized by assigning suitable ID's and passwords and using an appropriate authentication step. It can be appreciated that the present invention could operate without any authentication step. But the present invention could be improved by including an authentication step. It is preferable to prevent a member of one group from accessing pricing assigned or targeted for other groups; however, it can be appreciated that a vendor could grant access to either some or all members from one group to decryption keys that are assigned to another group which may improve flexibility and convenience for managing customer relations.

Referring to Fig. 1 which shows how to provide access to pricing (10) under scenario (B), a vendor freely provides retail pricing to anyone (14) that can access the vendor's web server while granting access to pricing (12) assigned to authenticated members (18) of a group after performing an authentication step (16). If an authentication step (16) is not successful, a customer is denied access to encrypted pricing (20). Ideally, group-assigned pricing should not be accessible by members belonging to other groups, unauthorized customers, or competitors; however, it can be appreciated that group-targeted pricing could be made accessible to members

of more than one group which may improve the management of customer relations. The present invention can be further adapted so that members of wholesale and/or favourable customer groups are granted access to their group-targeted pricing in which the pricing or decryption key is not made accessible to non-members. Customers are not required to register and authenticate themselves (12, 14); however, customers who are authenticated members of a group could preferably be identified and authenticated (16, 18) prior to granting access to pricing. The present invention determines to which group a customer member (22) belongs. At least two public-private key pairs are required in which one key pair is assigned to a first group, such as a wholesale group, and another key pair is assigned to a second group, such as a favourable customer group. Authenticated members of a group are granted access to an assigned public key (24) along with assigned encrypted pricing (26) so that the decryption key can be used to decrypt the encrypted pricing (28).

In a similar fashion to scenario (A), a vendor avoids generating or managing a unique key pair for specific customers by assigning key pairs to groups of customers. Preferably, members of one group should not be able to access granted to the pricing that is targeted and encrypted for other assigned groups.

Referring to Fig. 2, it is shown how to grant access to group-targeted pricing. The steps include:

Step 1. Define specific groups of members and place customers into a specific group in which for this example there are N groups (30);

Step 2. Determine which groups will have access to encrypted pricing in which for this example there are M groups and that M is less than N (32);

Step 3. Assign a pricing strategy to each group in which the pricing strategy contains pricing for one product or a range of products; preferably, there are at least a total of M pricing strategies that will be encrypted; however, it can be appreciated that some groups could share a pricing strategy which may improve the management of customer relations;

Step 4. Create a public-private key pair for each group in which there are up to M key pairs (34);

Step 5. Assign a public-private key pair to each customer group (36);

Step 6. Encrypt pricing strategies by using a private key of a public-private key pair that is assigned to a group (38);

Step 7. Prevent private keys from being accessed by customers and allow assigned public keys to be accessed by authenticated members of a group (40);

Step 8. Grant access to a group-assigned public key and group-assigned encrypted pricing to an authenticated member so that the group-assigned public key can be used to decrypt the encrypted pricing (42); and

Step 9. Display decrypted pricing on a customer's web browser.

The present invention provides an advantage by reversing usage of public-private key pairs for protecting information. An aspect of the present invention uses a private key of a public-private key pair to encrypt group-assigned pricing and a group-assigned public key is used to decrypt an encrypted group-assigned pricing. Key management becomes a minimal task since a number of groups is usually smaller that a total number of customers. While a vendor may potentially have to manage requests from potentially millions of customers over the Internet,

there will be a significantly smaller number of customer groups that will be relatively easier to manage.

It can be appreciated that the present invention can be further adapted to be incorporated in a computer program that contains executable software instructions for implementing the concepts of the present invention in which the program can be used on a general purpose computer or a web server over a communications network such as the Internet. It can be appreciated that a distribution mechanism can be used to distribute the computer program in which the distribution mechanism allows the vendor to access the computer program. The distribution mechanism or media could be a computer media such as a floppy disk, compact disk, and the like. Additionally, the distribution mechanism could be software instructions that can be downloaded over a network, such as the Internet in which the downloaded instructions incorporate the software instructions that execute the concepts of the present invention.

It can be appreciated that the concepts of the present invention can be further extended to a variety of other applications that are clearly within the scope of this invention in which users or customers can access many types of assigned information such as press releases, temporary pricing, warranty information and the like, in addition to or instead of pricing information.

Having thus described the present invention with respect to a preferred embodiment as implemented for granting access to group-targeted pricing information to members of groups, it will be apparent to those skilled in the art that many modifications and enhancements are possible to the present invention without departing from the basic concepts as described in the preferred embodiment. Therefore, what is intended to be protected by way of letters patent is set forth in the following claims as description and not limitation.

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A controlled access catalog for storing identification of catalog items accessible by members of authorized groups, said catalog containing:

a) identification of an authorized group;

b) identification of selected catalog items and group information for said authorized group, and a private key of said authorized group for encrypting said group information;

c) a public key for said authorized group for decrypting encrypted group information, said public key corresponding respectively to said private key of said authorized group; and

d) authentication means for granting access to said public key of said authorized group for decrypting said encrypted group information for members of said authorized group.

2. A controlled access catalog for storing identification of catalog items accessible by members of authorized groups, said catalog containing:

   a) identification of said authorized groups;

   b) identification of selected catalog items and group information for each authorized group, and a private key of said each authorized group for encrypting said group information;

   c) a public key for each said authorized group for decrypting encrypted group information, each said public key corresponding respectively to a private key of each said authorized group; and

   d) authentication means for granting access to said public key of each said authorized group for respectively decrypting encrypted group information of each said authorized group for its members.

3. The catalog of claim 1 wherein said authentication means is responsive to receiving member identification for granting access to said public key of said authorized group.

4. The catalog of claim 1 wherein said group information includes group pricing.

5. The catalog of claim 4 further comprising decryption means for decrypting encrypted group pricing using said public key when pricing information is requested by an authenticated member of said authorized group.

6. The catalog of claim 5 further comprising identification of said members of said authorized group.

7. The catalog of claim 6 further comprising:

   a) encryption means for encrypting said group pricing by using said private key; and

   b) access means for accessing said encrypted group pricing of said authorized group by said members, said access means being responsive to a member providing identification and authentication data for confirming authorization of said member to access said encrypted group pricing.

8. A multinodal information-handling network including said catalog of claim 7 at a first node of said network.

9. User interface means at a second node of said network of claim 8, said user interface means comprising:

   a) input means for accepting member input, including member identification and authentication data;

   b) communication means for sending said member input from said second node to said catalog over said network.

10. The user interface means of claim 9 wherein said communication means is adapted to receive information output from said catalog including identification of catalog items and decrypted group pricing, and said interface means comprises presentation means to display, for a user, identification and pricing of said catalog items.

11. The user interface of claim 10 wherein said presentation means is adapted to present to a user:

a) an input screen having an input field for said user to enter a query including member identification and authentication data to be sent to said catalog by said communication means to request access to said catalog; and

b) a user presentation screen to display information including decrypted pricing of catalog items available to said user after access to said catalog has been communicated to said communication means.

12. A method for managing a controlled access catalog for storing identification of catalog items accessible by members of authorized groups, comprising:

a) storing identification of an authorized group;

b) storing identification of selected catalog items and group information for said authorized group;

c) encrypting said group information with a private key of said authorized group;

d) storing a public key for said authorized group for decrypting encrypted group information, said public key corresponding to said private key of said authorized group; and

e) authenticating and granting access to said public key of said authorized group for decrypting said encrypted group information for members of said authorized group.

13. The method of claim 11 wherein the step of authenticating is responsive to receiving member identification, for granting access to said public key of said authorized group.

14. The method of claim 11 wherein said group information includes group pricing.

15. The method of claim 14 further comprising decrypting encrypted group pricing using said public key when pricing information is requested by an authenticated member of said authorized group.

16. The method of claim 15 further comprising storing identification of said members of said authorized group.

17. The method of claim 16 further comprising:

a) encrypting said group pricing of an authorized group by using said private key of said authorized group; and

b) providing access to said encrypted group pricing of said authorized group, responsive to a user providing identification and authentication data for confirming authorization of said member to access said encrypted group pricing.

18. A program product having a computer-readable medium storing computer-readable program code for managing a controlled access catalog accessible by members of authorized groups, said program code comprising:

a) computer-readable program code for causing said computer to store identification of an authorized group;

b) computer-readable program code for causing said computer to store identification of selected catalog items and group information for said authorized group;

c) computer-readable program code for causing said computer to encrypt said group information with a private key of said authorized group;

d) computer-readable program code for causing said computer to store a public key for said authorized group for decrypting encrypted group information, said public key corresponding respectively to said private key of said authorized group; and

e) computer-readable program code for causing said computer to authenticate and grant access to said public key of said authorized group for decrypting said encrypted group information for a member of said authorized group.

19. The product of 18 wherein the computer-readable program code for causing said computer to authenticate is responsive to receiving member identification.

20. The product claim 18 wherein said group information includes group pricing.

21. The product of claim 20 further comprising computer-readable program code for causing said computer to decrypt encrypted group pricing using said public key when pricing information is requested by an authenticated member of said authorized group.

22. The product of claim 21 further comprising computer-readable program code for causing said computer to store identification of said members of said authorized group.

23. The product of claim 22 further comprising computer-readable program code for causing said computer to access said encrypted group pricing of said authorized group by said members, responsive to a member providing identification and authentication data for confirming authorization of said member to access said encrypted group pricing.

Figure 1

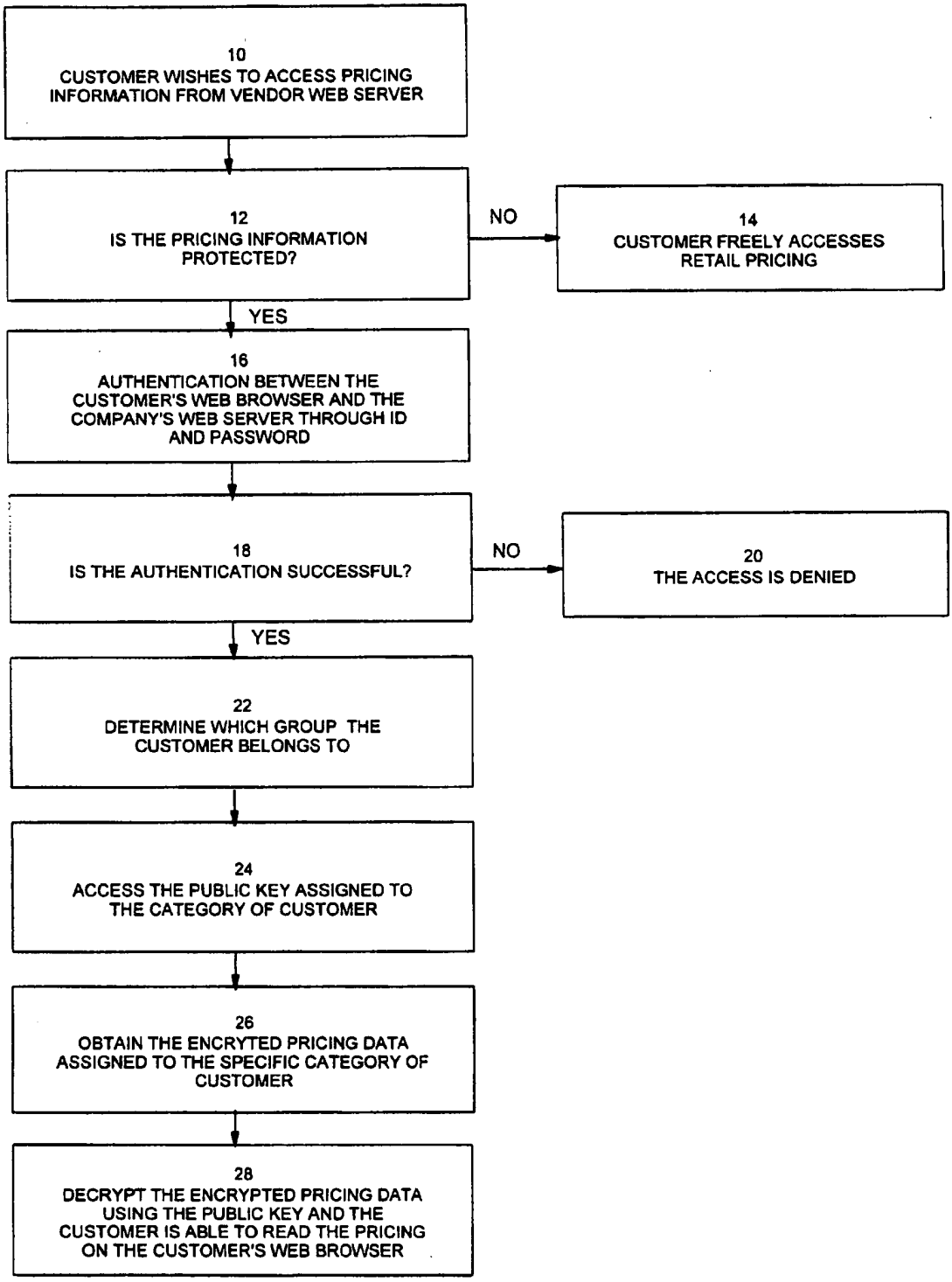
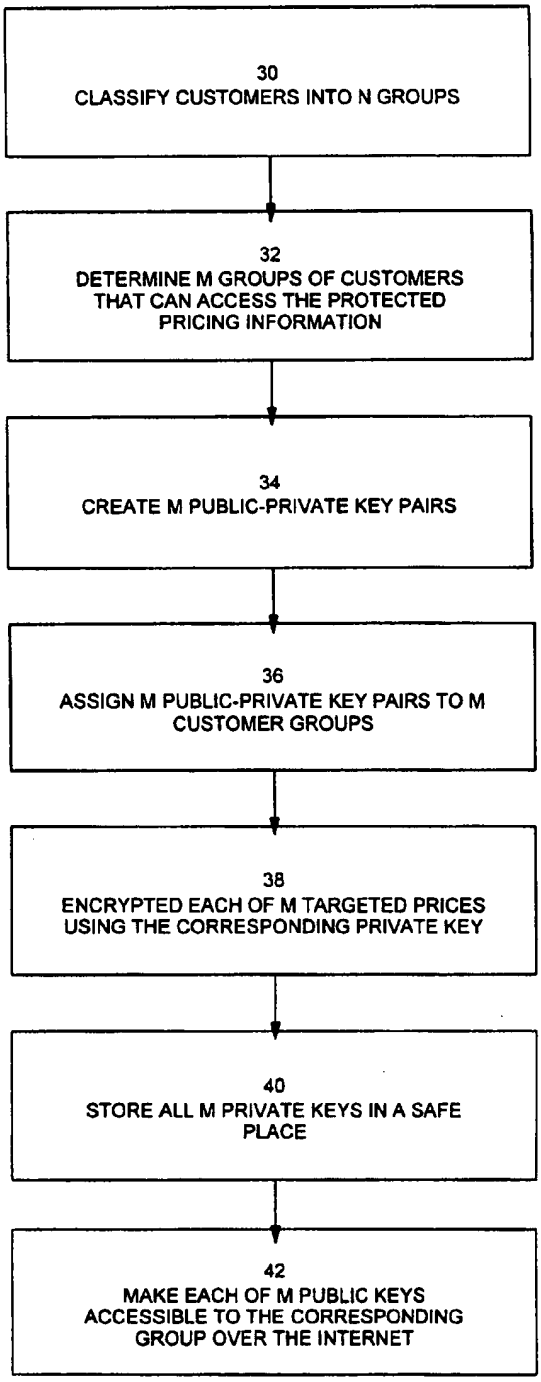

10
CUSTOMER WISHES TO ACCESS PRICING INFORMATION FROM VENDOR WEB SERVER
12
IS THE PRICING INFORMATION PROTECTED?
NO
14
CUSTOMER FREELY ACCESSES RETAIL PRICING
YES
16
AUTHENTICATION BETWEEN THE CUSTOMER'S WEB BROWSER AND THE COMPANY'S WEB SERVER THROUGH ID AND PASSWORD
18
IS THE AUTHENTICATION SUCCESSFUL?
NO
20
THE ACCESS IS DENIED
YES
22
DETERMINE WHICH GROUP THE CUSTOMER BELONGS TO
24
ACCESS THE PUBLIC KEY ASSIGNED TO THE CATEGORY OF CUSTOMER
26
OBTAIN THE ENCRYTED PRICING DATA ASSIGNED TO THE SPECIFIC CATEGORY OF CUSTOMER
28
DECRYPT THE ENCRYPTED PRICING DATA USING THE PUBLIC KEY AND THE CUSTOMER IS ABLE TO READ THE PRICING ON THE CUSTOMER'S WEB BROWSER

Figure 2


30
CLASSIFY CUSTOMERS INTO N GROUPS
32
DETERMINE M GROUPS OF CUSTOMERS THAT CAN ACCESS THE PROTECTED PRICING INFORMATION
34
CREATE M PUBLIC-PRIVATE KEY PAIRS
36
ASSIGN M PUBLIC-PRIVATE KEY PAIRS TO M CUSTOMER GROUPS
38
ENCRYPTED EACH OF M TARGETED PRICES USING THE CORRESPONDING PRIVATE KEY
40
STORE ALL M PRIVATE KEYS IN A SAFE PLACE
42
MAKE EACH OF M PUBLIC KEYS ACCESSIBLE TO THE CORRESPONDING GROUP OVER THE INTERNET